

Remarks and Arguments

Applicant's attorney wishes to thank the examiner for his time during a telephonic interview conducted on December 28, 2004. During that interview, the cited Ganesan and Linehan references were discussed together with the differences between the disclosure of these references and the claimed limitations. The substance of that interview is set forth in detail below.

The claimed invention in the present application is a system and method for transmitting information from a client to a file server and storing that information on the file server, where the information is secret and both the file server and the mechanism for transmitting the information from the client to the file server are not secure. According to the claimed technique, the information is first encrypted at the client with a first key. The first key is then encrypted at the client with a second key known to the client. Then the encrypted information and the encrypted first key are sent to the file server. At the file server, the encrypted information is stored and the encrypted first key is stored in an access table entry that contains a client ID identifying the client, the encrypted first key and information identifying where the information is stored.

The use of an access table allows other parties to access the information even if they did not store the information on the file server in the first place as long as they have the second key. In order to allow another party to access the information, an additional ID for that party is stored in a list in the access table entry. This additional ID identifies the other party.

When someone requests the information from the file server, they send their ID to the file server. The server then looks up the ID in the access table and returns the encrypted information and the access table entry that includes the ID. This latter entry includes the encrypted first key and the ID list. When the requesting party receives the information and the entry, it extracts the encrypted first key and then uses it to decrypt the encrypted information. For example, claim 1 recites "in response to a request from said client; transmitting to said client said encrypted information and said entry."

It should be noted that both encryption and decryption of the information is performed at the client. The client also generates the first and second keys so that no

key server is necessary. All information passing to and from the file server, including the information itself and any keys necessary to decrypt that information, is encrypted.

Regarding the rejection of claims 31-34 as anticipated by Ganesan, the recited retrieval operation is clearly recited in claim 31. Claim 31 recites in response to an information retrieval request, “receiving from said file server said information encrypted with a first encryption key having an associated first decryption key ...” and an “entry associated with a client authorized to at least read said information, ...including said first decryption key encrypted with a second encryption key having an associated second decryption key ...that is accessible to said client “

This is in contrast to the arrangement disclosed in Ganesan. In Ganesan, the client and the server first exchange encrypted requests for the stored information (steps 500 - 570, Figure 5) to insure that the request is from the proper party. Then the server retrieves an encrypted crypto-key and encrypted data from storage (580). Note that the crypto-key has been encrypted with an encryption key that is known to the server not the client. Thus, the server decrypts this crypto-key key using its own private key (585). The server uses the crypto-key to decrypt the information (590) and then sends the plaintext information to the client (595.) Thus, Ganesan does not disclose that the client receives from the server “...said information encrypted with a first encryption key having an associated first decryption key ...” as recited in claim 31. Further, the client does not receive a “first decryption key encrypted with a second encryption key having an associated second decryption key ...that is accessible to said client “also as recited in claim 31. Thus, claim 31 patentably distinguishes over the Ganesan reference.

Claims 35-37 have been rejected as anticipated by Linehan. The Linehan reference discloses a method for securely storing encrypted data. Linehan uses both a key server and a file server. When a client wants to store a file on the file server it sends an ID (a “ticket” as described in Linehan) to the key server together with the file name. The key server then generates an encryption key, stores the key and file name and sends the key back to the client. The client then encrypts the information with the key and sends the encrypted information to the file server where it is stored. Thus, the unencrypted key is stored on the key server and the encrypted data is stored in the file server. This arrangement differs from that recited in claim 35. Claim 35 recites

program code for storing on the file server “information encrypted with a first encryption key having a corresponding first decryption key that is usable to decrypt said encrypted information ” and an entry including “said first decryption key encrypted with a second encryption key associated with one of a plurality of clients authorized to at least read said information ” In Linehan, the key used to encrypt the information stored on the file server is not stored in encrypted form, either in the file server as recited or in the key server of Linehan. Linehan does suggest that the encryption key could be transmitted to the client encrypted with a session key (column 8, lines 20-23.) However, the information encryption as encrypted with the session key is clearly not stored on the file server with the information as recited in claim 35 or, for that matter, on the key server. Thus, claim 35 patentably distinguishes over the cited Linehan reference.

Claims 1, 4-7 and 13-18 were rejected as obvious over the combination of Ganesan and Linehan. In the first place, it is difficult to ascertain how these references can be combined since they operate in a completely different fashion. For example, as mentioned above, in Ganesan, file encryption is performed at the file server, whereas in Linehan, file encryption is performed at the client. This difference results in different keys being stored in different locations and different keys being used. However, even assuming that the reference could and should be combined, the resulting combination cannot teach or suggest the claimed invention. For example, claim 1 is representative. It recites storing at the file server “(i) information encrypted with a first encryption key and (ii) ... an entry that includes an identifier for a client authorized to at least read said encrypted information and a first decryption key encrypted with a second encryption key ...that is accessible to the client.” As noted above, Ganesan stores the file encryption key at the file server encrypted with a key that is accessible to the file server, not the client. Linehan does not store the encrypted file encryption key (presumably, the key server is secure). Since, neither reference discloses the claimed limitation, the combination cannot teach or suggest the combination. Thus, claims 1, 4-7 and 13-18 patentably distinguish over the cited combination of references.

Claims 8-11 have been rejected over the combination of Ganesan and Linehan in view of Menezes. The Menezes reference is a page from a general handbook on cryptography. Thus, its incorporation into the combination of Ganesan and Linehan

cannot change the basic operation of the Ganesan and Linehan combination. Claims 8-11 are dependent on claim 1 and incorporate its limitations. Since the Ganesan and Linehan combination does not teach or suggest the limitations of claim 1, adding Menezes to the combination cannot create the required teaching or suggestion.

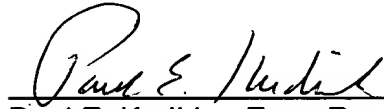
Claim 12 was rejected over the combination of Ganesan, Linehan, Menezes and Carter. Carter discloses a method and apparatus for controlling collaborative access to a work group document by the users of a computer system. The document has an encrypted data portion and a prefix portion. Data structures in the prefix portion are used to restrict access to the information stored in the data portion. However, in Carter users do not access the data over unsecure communication links. Thus, Carter is not concerned with passing plaintext information over those links. Consequently, Carter, as Ganesan performs encryption and decryption of the data at the server. Thus, its addition cannot change the basic operation of the Ganesan, Linehan and Menezes combination. Claim 12 depends indirectly on claim 1 and incorporates its limitations. Since the Ganesan, Linehan and Menezes combination does not teach or suggest the limitations of claim 1, adding Carter to the combination cannot create the required teaching or suggestion.

Claim 20-30 were rejected over the combinations of Eldridge and either Linehan or Ganesan. Eldridge is similar to Carter in that users do not access the data over unsecure communication links. Thus, Eldridge is not concerned with passing plaintext information over those links. Consequently, Eldridge, as Ganesan performs encryption and decryption of the data at the server. Thus, its addition cannot change the basic operation of Ganesan or Linehan. Claims 20 and 21 contain limitations that parallel those in claim 1. Since neither Ganesan nor teach or suggest the limitations of claim 1, adding Eldridge to the combination cannot create the required teaching or suggestion. The remainder of claims 20-30 dependent either on claim 21 and therefore distinguish over the cited combination in the same manner as claim 21.

In light of the forgoing remarks, this application is now believed in condition for allowance. Reconsideration of the claims and a notice of allowance is earnestly solicited. If the examiner has any further questions regarding this amendment, he is invited to call applicants' attorney at the number listed below. The examiner is hereby

authorized to charge any fees or direct any payment under 37 C.F.R. §§1.17, 1.16 to
Deposit Account number 02-3038.

Respectfully submitted



Date: 1/7/05

Paul E. Kudirka, Esq. Reg. No. 26,931

KUDIRKA & JOBSE, LLP

Customer Number 021127

Tel: (617) 367-4600 Fax: (617) 367-4656